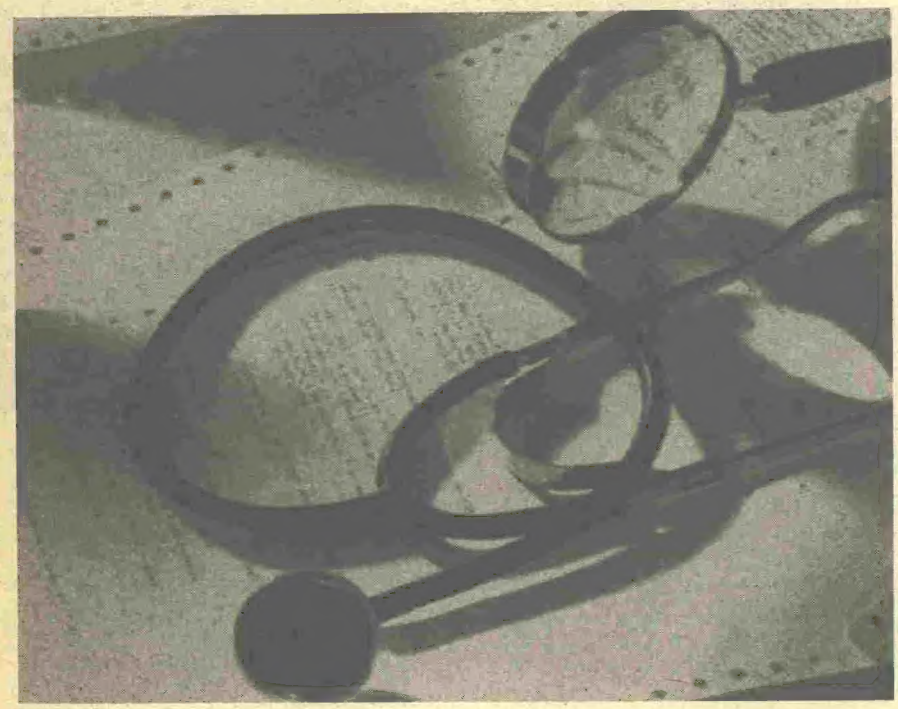
ศรันย์ ไมตรีเวช

ไวรัสบนไฟล์ .DOC

SOFT MAIL



หนามยอกต้องเอาหนามบ่ง ด้วยวิธีการปราบปรามที่มาในรูปของไฟล์ .DOC สำหรับไวรัสพันธุ์ใหม่ที่มากับไฟล์ .DOC เพ่นพ่านผ่านอินเทอร์เน็ต

คงต้องหนาวกันอีกรอบแล้วล่ะครับกับเรื่องของไวรัส ซึ่งผู้ใช้คอมพิวเตอร์ทั้งเกลียดทั้งกลัว เพราะคราวนี้มันไม่ได้มากับเงามืดของไฟล์ .EXE หรือ .DLL แต่มากับไฟล์ .DOC ซึ่งเป็นเอกสารทั่วไป และมีความเคลื่อนไหวจากเครื่องโน้นไปเครื่องนี้ถี่กว่าไฟล์จำพวกที่เป็นโปรแกรมสำเร็จมากนัก นั่นหมายความว่า โอกาสที่จะเกิดความปั่นป่วนวุ่นวายนั้นมีมากขึ้นอย่างเป็นที่ชวนผวายิ่ง

ในปัจจุบันไวรัสพันธุ์ใหม่นี้จะให้ผลกับผู้ใช้ไมโครซอฟต์เวิร์ด 6.0 เท่านั้น อย่างไรก็ตาม นี่คือยุคใหม่ของไวรัส เป็นยุคที่ฝันร้ายกลายเป็นจริง เรื่องเป็นไปไม่ได้มันเป็นไปแล้ว จากที่เคยให้ผลเฉพาะไฟล์โปรแกรม เดี๋ยวนี้ไฟล์เอกสารก็ไม่เว้น ต่อไปก็น่าคิดว่าจะไม่มีข้อยกเว้นอะไรอีก เนื่องจากมีโปรแกรมเมอร์นิสัยเสีย แถมเวลาว่างเยอะ สำแดงผลงานให้เพ่นพ่านผ่านอินเทอร์เน็ตไม่เว้นแต่ละวัน

เป็นที่ยืนยันแล้วด้วยนะครับว่าไวรัสพันธุ์นี้กระจายผ่านได้แม้กระทั่งอีเมล์ นั่นหมายความว่า คุณที่ใช้อินเทอร์เน็ตอยู่คงนิ่งนอนใจไม่ได้อีกต่อไป

มีการวิเคราะห์ไวรัสพันธุ์ใหม่นี้ และพบว่าผู้แพร่มันออกมา ได้ใช้เทคนิคพิเศษซึ่งไม่เคยปรากฏมาก่อน ฉายาอันเป็นที่รู้จักของมันคือวินเวิร์ดคอนเส็ปต์ (Winword.Concept) บางคนเรียกในเชิงเทคนิคว่า WW6Macro, WW6Infector, WBMW หรือ Prank Macro Virus ก็มี

นอกจากวินเวิร์ดคอนเส็ปต์แล้ว เท่าที่ทราบตอนนี้ยังมีอีกพันธุ์หนึ่งชื่อวินเวิร์ดดีเอ็มวี-เดโม (WinWord.DMV-Demo) หรือเรียกสั้น ๆ ว่า DMV สำหรับพันธุ์ใหม่ที่ตามหลังพันธุ์แรกมานี้ ผมยังไม่ทราบครับว่ามันจะออกฤทธิ์ท่าไหน แต่ในส่วนวินเวิร์ดคอนเส็ปต์นั้น มันสามารถสำแดงเดชได้หลายแพลตฟอร์ม ไม่ว่าจะเป็นวินโดวส์ 3.x วินโดวส์ 95 วินโดวส์เอ็นที หรือกระทั่งเครื่องแมคอินทอช อะไรก็แล้วแต่ที่รันไมโครซอฟต์เวิร์ด 6 ได้ล่ะก็ นั่นแหละครับที่ใช่

ไวรัสวายร้ายตัวนี้ใช้ช่องทางของภาษาแมคโครของวินเวิร์ดในการแพร่พันธุ์เข้าไปในไฟล์เอกสารและ NORMAL.DOT ซึ่งมักใช้เป็นเทมเพลตดีฟอลต์ของเวิร์ด 6

เมื่อเอกสารที่ติดไวรัสถูกเปิดขึ้นโดยสภาพแวดล้อมของไมโครซอฟต์เวิร์ดในครั้งแรก ไวรัสจะเข้าทำการรู่โจมในรูปของแมคโคร AutoOpen และแพร่พันธุ์เข้าไปในเทมเพลต NORMAL.DOT หรือเทมเพลตโกลบอลอื่นใดที่ถูกกำหนดให้เป็นดีฟอลต์

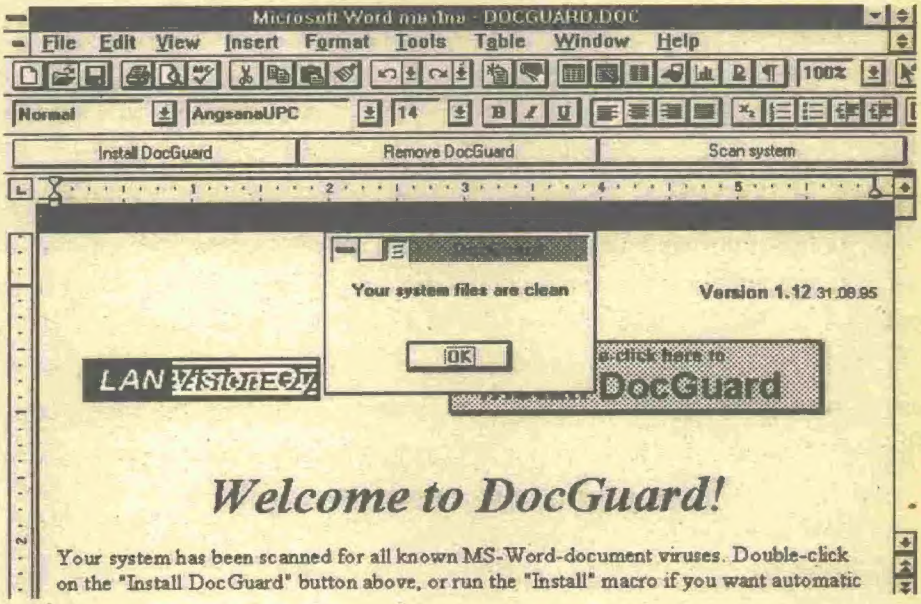
หากคุณเป็นผู้โชคไม่ดี เจอแจ็คพ็อตเข้าล่ะก็ คุณจะได้พบกับเมสเสจบ็อกซ์ปรากฏบนหน้าจอ แสดงตัวเลข "1" (อันนี้เป็นการแผลงฤทธิ์เท่าที่พบขณะผมกำลังเขียนบทความอยู่นะครับ แน่นอนว่าคงเกิดเรื่องราวพิสดารยิ่งกว่านี้ในเวลาต่อ ๆ ไป)

จากนั้นไม่ว่าไฟล์ใดก็ตามที่จะถูกนำขึ้นมาแก้ไขแล้วจัดเก็บด้วยสภาพแวดล้อมของไมโครซอฟต์เวิร์ด ก็จะพลอยถูกแพร่พันธุ์ไปด้วยอย่างหลีกเลี่ยงไม่ได้ โดยวิธีนี้คุณจะเห็นว่าไม่ใช่เรื่องสนุกเลยถ้าหากไฟล์เข้าปัญหาถูกนำไปเข้าเครื่องสักยี่สิบเครื่อง มีคนสักสามคนเข้ามาใช้วินเวิร์ดของแต่ละเครื่องต่อวัน (ซึ่งแน่นอนว่าเขาเหล่านั้นจะต้องนำไฟล์ไปเปิดที่อื่นส่งต่อให้คนอื่นด้วย) คุณอาจดูได้ด้วยตัวเองว่าไมโครซอฟต์เวิร์ดของคุณเจอตลกร้ายรายการนี้แล้วหรือยัง ด้วยการเปิดลิสต์แมคโคร (โดยเลือกเมนู Tools...Macros) แล้วเช็คดูว่ามีแมคโครชื่อ AAAZFS, AAAZAO, AutoOpen, Payload, และ FileSaveAs อยู่ในลิสต์หรือเปล่า หากพบตามนี้ล่ะก็ เป็นอันว่าคุณกำลังมีปัญหาและอาจจะเคยแพร่ปัญหาออกไปในวงกว้างโดยไม่รู้เนื้อรู้ตัวแล้วล่ะครับ

พฤติกรรมร้าย ๆ ของวินเวิร์ดคอนเส็ปต์นั้น เท่าที่พบในปัจจุบันอยู่ในรูปของปัญหาในการจัดเก็บไฟล์ แต่ยังไม่หนักหนาขนาดทำลายระบบเหมือนอย่างไวรัสตัวอื่น อย่างไรก็ตาม ผู้ใช้ไฟล์เอกสารเราท่านทั่วไปคงไม่สบายใจแน่เมื่อทราบถึงปรากฏการณ์ชนิดนี้ เนื่องจากไฟล์เอกสารบางไฟล์นั้นสูญเสียไม่ได้ ผิดพลาดประการใด ๆ ไม่ได้ทั้งสิ้น (ป่วยการคิดถึงไฟล์สำรอง เนื่องจากหากไฟล์ต้นฉบับมีสิ่งผิดปกติเข้าแล้ว จะคัดลอกไว้สักกี่สำเนาก็เหมือนกันหมด)

ยังดีครับที่โลกนี้มีทั้งวายร้ายและพระเอกปะปนกันอยู่ ไม่ได้เป็นโลกของวายร้ายเสียฝ่ายเดียว ดังนั้นจึงมีผู้คิดค้นวิธีป้องกันด้วยวิธีที่ผู้ใช้ทั่วไปสามารถติดตั้งกับเครื่องของตนเองได้โดยง่าย

อุปกรณ์ป้องกันและปราบปรามไวรัสไฟล์เอกสารที่ว่านี้ มาในรูปของไฟล์เอกสาร



รูปที่ 1

นั่นแหละ เข้าทำนองหนามยอกเอาหนามบ่งชื่อไฟล์คือ Docguard.DOC ผลิตโดยบริษัท LAN Vision Oy เขียนโดย M.Albrecht คุณสามารถโหลดมันขึ้นมาได้เสมือนเป็นไฟล์เอกสารทั่วไป ที่พิเศษคือ เมื่อโหลดเรียบร้อยแล้วมันจะทำการสแกนระบบให้คุณ แล้วบอกให้ทราบทันทีว่าตอนนี้ในระบบของคุณมีไวรัสติดอยู่หรือเปล่า ดังรูปที่ 1

เมื่อคลิ๊ก Ok จะเห็นว่าคุณเข้าสู่โหมดของการแก้ไขเอกสารตามปกติ สังเกตนะครับว่าจะมีทูลบาร์ใหม่ขึ้นมาบรรทัดหนึ่ง อันนั้นคือ Docguard Toolbar นั่นเอง คุณสามารถทำให้มันหายไปหรือกลับปรากฏได้ด้วยเมนูคำสั่ง View...Toolbars เสมือนเป็นทูลบาร์ทั่วไป

ด้วย Docguard Toolbar นี้ คุณสามารถติดตั้งระบบตรวจสอบอัตโนมัติ เพียงคลิ๊กปุ่ม Install Docguard ปุ่มเดียว หมายความว่าต่อไปไม่ว่าคุณจะโหลด Docguard.DOC ขึ้นมาหรือไม่ ก็จะมีการตรวจสอบเสมอว่าไฟล์เอกสารที่คุณโหลดมาแก้ไขนั้นติดไวรัสมาหรือเปล่า หากติดมาก็จะทำการ "ทำความสะอาด" หรืออีกนัยหนึ่งคือฆ่าไวรัสทิ้งให้ทันทีโดยอัตโนมัติ

หากคุณไม่พอใจ ก็อาจนำระบบตรวจสอบอัตโนมัติของ Docguard ออกไปก็ได้ด้วยปุ่ม Remove Docguard และหากจะตรวจสอบระบบด้วยตนเอง ก็เพียงคลิ๊กปุ่ม Scan System

สำหรับคนที่ไม่ค่อยรู้เรื่องเกี่ยวกับทูลบาร์ หรือเห็นปุ่มบนทูลบาร์ได้ยาก ทาง LAN Vision Oy ก็ได้ตระเตรียมพื้นที่สำหรับดับเบิลคลิ๊กใหญ่ ๆ มาให้ ก็ที่เห็นสะดุดตาว่า Double-click here to Install Docguard ตรงมุมบนขวามือนั่นแหละครับ มีค่าเท่ากับคลิ๊กปุ่ม Install Docguard บน Docguard Toolbar

การติดตั้ง Docguard นั้นหมายถึง การคัดลอกแมคโครสามตัว คือ AutoExec, Auto Open และ FileOpen เข้าไปไว้ในเทมเพลต NORMAL.DOT ที่ต้องบอกให้ทราบไว้ก็เผื่อคุณไปดูลิสต์แมคโครแล้วเห็นมีอะไรเพิ่มเข้ามาผิดปกติ เกิดไปลบออกเข้าล่ะก็ เป็นอันว่าขามรักษาการความปลอดภัยจากไวรัสตัวเก่งถูกปลดระวางไปทันที

คุณอาจเกิดความเป็นห่วงขึ้นมาว่า แล้วแมคโครเก่าที่มีชื่อซ้ำกันล่ะ จะเป็นอย่างไร อันนี้ก็สบายใจได้ครับ Docguard จะจัดการเปลี่ยนชื่อพวกมันให้กลายเป็น DocGuardSaved (ยกเว้น FileOpen จะไม่มีการทำอย่างนั้น อันนี้เป็นเรื่องทางเทคนิคเกี่ยวกับความปลอดภัย เพราะแมคโคร FileOpen นี่แหละครับที่เป็นหน้าด่านสำคัญในการทำลายหรือป้องกัน)

สำหรับไฟล์ที่เปิดขึ้นมาล่าสุดซึ่งจะถูกเก็บไว้ให้คุณเห็นในเมนู File ตอนล่างนั้น จะไม่สามารถได้รับการสแกนจาก Docguard นอกจากนั้นลิสต์ของไฟล์เหล่านี้ยังอาจถูกถอดทิ้งอีกด้วย เพราะหากคุณใช้เมนูคำสั่งในการเรียกไฟล์เหล่านี้ (แทนที่จะใช้วิธี Open File) พวกมันจะถูกละเลย ไม่อาจสแกนให้แน่ใจจาก Docguard ว่าพวกมันสะอาดจากไวรัสหรือเปล่า วิธีที่ดีที่สุดคือ คุณควรทำให้ลิสต์ไฟล์ล่าสุดหายไปด้วยเมนูคำสั่ง Tools...Options... General แล้วกลับมาใช้ใหม่หลังจากติดตั้ง Docguard เรียบร้อยแล้ว ซึ่งเป็นประกันว่าต่อไปทุกไฟล์ที่ตามหลังมาจะถูก Docguard สแกนเสียก่อนใช้

อีกประการหนึ่งที่สำคัญคือ Docguard จะไม่อาจได้รับการติดตั้งหากเทมเพลต NORMAL.DOT ถูกเปิดใช้ในโหมด read only (ห้ามเขียนทับ) คุณจะต้องเอา write protect ออกเสียก่อนที่จะติดตั้งนะครับ

สำหรับ Docguard.DOC นี้ เป็นไฟล์ที่คุณสามารถเรียกหาได้จากซอฟต์แมล์ของไมโครคอมพิวเตอร์ และถ้าหากใครเข้าบีบีเอส Green Leaf (746-1088, 399-2616) ได้ ก็สามารถไปนำไฟล์นี้มาโดยตรง เนื่องจากมีคนอัพโหลดไปไว้ที่นั่นเรียบร้อยแล้ว

แน่นอนว่าต่อไปนี้การใช้งานคอมพิวเตอร์คงอันตรายขึ้นอีกเยอะ หากต้องการติดต่อกับพระเอกผู้ช่วยเหลือของเราโดยตรง ก็ให้ติดต่อผ่านอินเทอร์เน็ตไปตามนี้

```
e-mail:     buster@klaine.pp.fi
FTP:   ftp://ftp.lanvision.fi/pub/ww6macro
URL:   http://ftp.lanvision.fi/lanvision.html
```

ชื่อของคนที่คุณจะติดต่อด้วยคือ Albrecht ขอให้โชคดีครับ อย่าต้องมาเจอไวรัสอะไรกันเลย ผมเองเจอมาจนงานเสียหายเสียเข็ดแล้ว เข้าใจหัวอกคนเคราะห์ร้ายเจอไวรัสด้วยกันเป็นอย่างดี หากมีความคืบหน้าอย่างไรจะพยายามมาบอกกล่าวให้ทราบทั่วกัน สวัสดี

รับสมัครด่วน

บริษัท มัชฌิมา คอมพิวเตอร์และโอเอ จำกัด ผู้นำเข้าอุปกรณ์คอมพิวเตอร์ทั้ง DATASTO- RAGE, MULTIMEDIA เช่น "TEAC" Remove-able Harddish CD-ROMx4, TAPE BACK-UP และอุปกรณ์สื่อสารไร้สาย รวมทั้ง WIRELESS MODEM ต้องการรับสมัครบุคลากรเพื่อร่วมงาน มีความกระตือรือร้น รักความก้าวหน้าในตำแหน่งต่อไปนี้

1. ***ผู้จัดการฝ่ายขาย*** 1 ตำแหน่ง
   ปริญญาตรีขึ้นไป มีประสบการณ์
2. ***พนักงานขาย และ SUPPORT*** 4 ตำแหน่ง
   ปวช-ปริญญาตรี
3. ***ช่างเทคนิค*** 2 ตำแหน่ง
   ปวส ขึ้นไป มีประสบการณ์ด้าน COMPUTER
4. ***พนักงานธุรการ*** 3 ตำแหน่ง
   ปวช-ปวส
5. ***พนักงานบัญชี*** 2 ตำแหน่ง
   ปวส-ปริญญาตรี

ทุกตำแหน่งถ้าประสบการณ์ด้านคอมพิวเตอร์จะได้รับพิจารณาเป็นพิเศษ ติดต่อด้วยตนเองได้ที่

บริษัท มัชฌิมา คอมพิวเตอร์และโอเอ จำกัด
เลขที่ 44/37-38 ถนนงามวงศ์วาน แขวงลาดยาว เขตบางเขน กรุงเทพฯ 10900
โทรศัพท์ : 5915275-7, 5807476-9, 5895273, 5911582 โทรสาร : 5894537